

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

| | | | |
|--|--|---|--|
| (51) Classification internationale des brevets ⁶ : H04L 9/06, 9/30 | | A1 | (11) Numéro de publication internationale: WO 99/48239 (43) Date de publication internationale: 23 septembre 1999 (23.09.99) |
| <p>(21) Numéro de la demande internationale: PCT/FR99/00613 (22) Date de dépôt international: 17 mars 1999 (17.03.99)</p> <p>(30) Données relatives à la priorité: 98/03242 17 mars 1998 (17.03.98) FR</p> <p>(71) Déposant (<i>pour tous les Etats désignés sauf US</i>): SCHLUM-BERGER SYSTEMES [FR/FR]; 50, avenue Jean Jaurès, F-92120 Montrouge (FR).</p> <p>(72) Inventeur; et (75) Inventeur/Déposant (<i>US seulement</i>): SALLE, Patrick [FR/FR]; 46, rue d'Amblainvilliers, F-91370 Verrières-le-Buisson (FR).</p> <p>(74) Mandataire: MACQUET, Christophe; Schlumberger Systèmes, Test & Transactions, Boite postale 620-04, F-92542 Montrouge Cedex (FR).</p> | | <p>(81) Etats désignés: AU, CA, CN, JP, US, brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).</p> <p>Publiée <i>Avec rapport de recherche internationale.</i></p> | |
| <p>(54) Title: METHOD FOR DATA SECUREMENT USING A CRYPTOGRAPHIC ALGORITHM</p> <p>(54) Titre: PROCEDE DE SECURISATION DE DONNEES METTANT EN OEUVRE UN ALGORITHME CRYPTOGRAPHIQUE</p> <p>(57) Abstract</p> <p>The invention concerns a method for data securement using a cryptographic algorithm comprising at least a cycle executing repetitive operations of processing data elements (K2, R1) to produce encrypted information (C), said method comprising at least a step (120, 220) randomly modifying the execution of at least one operation from one cycle to the next or at least one of the data elements such that the encrypted information is unaltered by said random modification.</p> <p>(57) Abrégé</p> <p>L'invention concerne un procédé de sécurisation de données mettant en oeuvre un algorithme cryptographique comprenant au moins un cycle d'exécution d'opérations répétitives de traitement d'éléments de données (K2, R1) pour élaborer une information chiffrée (C), ce procédé comprenant au moins une étape (120, 220) de modification aléatoire de l'exécution d'au moins une opération d'un cycle à un autre ou d'au moins un des éléments de telle sorte que l'information chiffrée soit inchangée par cette modification aléatoire.</p> | | | |
| <pre> graph TD M[Permutation du bloc Message M → M0] --> M0 K1[Permutation des bits de la clé K1 → K2] --> K2 M0 --> M1 M0 --> M2 K2 --> K3 K2 --> K4 K3 --> K4 K4 --> K5 M1 --> M3 M2 --> M3 M3 --> R1 R1 --> R2 R2 --> R3 R3 --> R4 R4 --> C R1 --> R5 R5 --> M1 R1 --> R6 R6 --> R7 R7 --> R8 R8 --> R9 R9 --> R10 R10 --> R11 R11 --> R12 R12 --> R13 R13 --> R14 R14 --> R15 R15 --> R16 R16 --> R17 R17 --> R18 R18 --> R19 R19 --> R20 R20 --> R21 R21 --> R22 R22 --> R23 R23 --> R24 R24 --> R25 R25 --> R26 R26 --> R27 R27 --> R28 R28 --> R29 R29 --> R30 R30 --> R31 R31 --> R32 R32 --> R33 R33 --> R34 R34 --> R35 R35 --> R36 R36 --> R37 R37 --> R38 R38 --> R39 R39 --> R40 R40 --> R41 R41 --> R42 R42 --> R43 R43 --> R44 R44 --> R45 R45 --> R46 R46 --> R47 R47 --> R48 R48 --> R49 R49 --> R50 R50 --> R51 R51 --> R52 R52 --> R53 R53 --> R54 R54 --> R55 R55 --> R56 R56 --> R57 R57 --> R58 R58 --> R59 R59 --> R60 R60 --> R61 R61 --> R62 R62 --> R63 R63 --> R64 R64 --> R65 R65 --> R66 R66 --> R67 R67 --> R68 R68 --> R69 R69 --> R70 R70 --> R71 R71 --> R72 R72 --> R73 R73 --> R74 R74 --> R75 R75 --> R76 R76 --> R77 R77 --> R78 R78 --> R79 R79 --> R80 R80 --> R81 R81 --> R82 R82 --> R83 R83 --> R84 R84 --> R85 R85 --> R86 R86 --> R87 R87 --> R88 R88 --> R89 R89 --> R90 R90 --> R91 R91 --> R92 R92 --> R93 R93 --> R94 R94 --> R95 R95 --> R96 R96 --> R97 R97 --> R98 R98 --> R99 R99 --> R100 R100 --> R101 R101 --> R102 R102 --> R103 R103 --> R104 R104 --> R105 R105 --> R106 R106 --> R107 R107 --> R108 R108 --> R109 R109 --> R110 R110 --> R111 R111 --> R112 R112 --> R113 R113 --> R114 R114 --> R115 R115 --> R116 R116 --> R117 R117 --> R118 R118 --> R119 R119 --> R120 R120 --> R121 R121 --> R122 R122 --> R123 R123 --> R124 R124 --> R125 R125 --> R126 R126 --> R127 R127 --> R128 R128 --> R129 R129 --> R130 R130 --> R131 R131 --> R132 R132 --> R133 R133 --> R134 R134 --> R135 R135 --> R136 R136 --> R137 R137 --> R138 R138 --> R139 R139 --> R140 R140 --> R141 R141 --> R142 R142 --> R143 R143 --> R144 R144 --> R145 R145 --> R146 R146 --> R147 R147 --> R148 R148 --> R149 R149 --> R150 R150 --> R151 R151 --> R152 R152 --> R153 R153 --> R154 R154 --> R155 R155 --> R156 R156 --> R157 R157 --> R158 R158 --> R159 R159 --> R160 R160 --> R161 R161 --> R162 R162 --> R163 R163 --> R164 R164 --> R165 R165 --> R166 R166 --> R167 R167 --> R168 R168 --> R169 R169 --> R170 R170 --> R171 R171 --> R172 R172 --> R173 R173 --> R174 R174 --> R175 R175 --> R176 R176 --> R177 R177 --> R178 R178 --> R179 R179 --> R180 R180 --> R181 R181 --> R182 R182 --> R183 R183 --> R184 R184 --> R185 R185 --> R186 R186 --> R187 R187 --> R188 R188 --> R189 R189 --> R190 R190 --> R191 R191 --> R192 R192 --> R193 R193 --> R194 R194 --> R195 R195 --> R196 R196 --> R197 R197 --> R198 R198 --> R199 R199 --> R200 R200 --> R201 R201 --> R202 R202 --> R203 R203 --> R204 R204 --> R205 R205 --> R206 R206 --> R207 R207 --> R208 R208 --> R209 R209 --> R210 R210 --> R211 R211 --> R212 R212 --> R213 R213 --> R214 R214 --> R215 R215 --> R216 R216 --> R217 R217 --> R218 R218 --> R219 R219 --> R220 R220 --> R221 R221 --> R222 R222 --> R223 R223 --> R224 R224 --> R225 R225 --> R226 R226 --> R227 R227 --> R228 R228 --> R229 R229 --> R230 R230 --> R231 R231 --> R232 R232 --> R233 R233 --> R234 R234 --> R235 R235 --> R236 R236 --> R237 R237 --> R238 R238 --> R239 R239 --> R240 R240 --> R241 R241 --> R242 R242 --> R243 R243 --> R244 R244 --> R245 R245 --> R246 R246 --> R247 R247 --> R248 R248 --> R249 R249 --> R250 R250 --> R251 R251 --> R252 R252 --> R253 R253 --> R254 R254 --> R255 R255 --> R256 R256 --> R257 R257 --> R258 R258 --> R259 R259 --> R260 R260 --> R261 R261 --> R262 R262 --> R263 R263 --> R264 R264 --> R265 R265 --> R266 R266 --> R267 R267 --> R268 R268 --> R269 R269 --> R270 R270 --> R271 R271 --> R272 R272 --> R273 R273 --> R274 R274 --> R275 R275 --> R276 R276 --> R277 R277 --> R278 R278 --> R279 R279 --> R280 R280 --> R281 R281 --> R282 R282 --> R283 R283 --> R284 R284 --> R285 R285 --> R286 R286 --> R287 R287 --> R288 R288 --> R289 R289 --> R290 R290 --> R291 R291 --> R292 R292 --> R293 R293 --> R294 R294 --> R295 R295 --> R296 R296 --> R297 R297 --> R298 R298 --> R299 R299 --> R300 R300 --> R301 R301 --> R302 R302 --> R303 R303 --> R304 R304 --> R305 R305 --> R306 R306 --> R307 R307 --> R308 R308 --> R309 R309 --> R310 R310 --> R311 R311 --> R312 R312 --> R313 R313 --> R314 R314 --> R315 R315 --> R316 R316 --> R317 R317 --> R318 R318 --> R319 R319 --> R320 R320 --> R321 R321 --> R322 R322 --> R323 R323 --> R324 R324 --> R325 R325 --> R326 R326 --> R327 R327 --> R328 R328 --> R329 R329 --> R330 R330 --> R331 R331 --> R332 R332 --> R333 R333 --> R334 R334 --> R335 R335 --> R336 R336 --> R337 R337 --> R338 R338 --> R339 R339 --> R340 R340 --> R341 R341 --> R342 R342 --> R343 R343 --> R344 R344 --> R345 R345 --> R346 R346 --> R347 R347 --> R348 R348 --> R349 R349 --> R350 R350 --> R351 R351 --> R352 R352 --> R353 R353 --> R354 R354 --> R355 R355 --> R356 R356 --> R357 R357 --> R358 R358 --> R359 R359 --> R360 R360 --> R361 R361 --> R362 R362 --> R363 R363 --> R364 R364 --> R365 R365 --> R366 R366 --> R367 R367 --> R368 R368 --> R369 R369 --> R370 R370 --> R371 R371 --> R372 R372 --> R373 R373 --> R374 R374 --> R375 R375 --> R376 R376 --> R377 R377 --> R378 R378 --> R379 R379 --> R380 R380 --> R381 R381 --> R382 R382 --> R383 R383 --> R384 R384 --> R385 R385 --> R386 R386 --> R387 R387 --> R388 R388 --> R389 R389 --> R390 R390 --> R391 R391 --> R392 R392 --> R393 R393 --> R394 R394 --> R395 R395 --> R396 R396 --> R397 R397 --> R398 R398 --> R399 R399 --> R400 R400 --> R401 R401 --> R402 R402 --> R403 R403 --> R404 R404 --> R405 R405 --> R406 R406 --> R407 R407 --> R408 R408 --> R409 R409 --> R410 R410 --> R411 R411 --> R412 R412 --> R413 R413 --> R414 R414 --> R415 R415 --> R416 R416 --> R417 R417 --> R418 R418 --> R419 R419 --> R420 R420 --> R421 R421 --> R422 R422 --> R423 R423 --> R424 R424 --> R425 R425 --> R426 R426 --> R427 R427 --> R428 R428 --> R429 R429 --> R430 R430 --> R431 R431 --> R432 R432 --> R433 R433 --> R434 R434 --> R435 R435 --> R436 R436 --> R437 R437 --> R438 R438 --> R439 R439 --> R440 R440 --> R441 R441 --> R442 R442 --> R443 R443 --> R444 R444 --> R445 R445 --> R446 R446 --> R447 R447 --> R448 R448 --> R449 R449 --> R450 R450 --> R451 R451 --> R452 R452 --> R453 R453 --> R454 R454 --> R455 R455 --> R456 R456 --> R457 R457 --> R458 R458 --> R459 R459 --> R460 R460 --> R461 R461 --> R462 R462 --> R463 R463 --> R464 R464 --> R465 R465 --> R466 R466 --> R467 R467 --> R468 R468 --> R469 R469 --> R470 R470 --> R471 R471 --> R472 R472 --> R473 R473 --> R474 R474 --> R475 R475 --> R476 R476 --> R477 R477 --> R478 R478 --> R479 R479 --> R480 R480 --> R481 R481 --> R482 R482 --> R483 R483 --> R484 R484 --> R485 R485 --> R486 R486 --> R487 R487 --> R488 R488 --> R489 R489 --> R490 R490 --> R491 R491 --> R492 R492 --> R493 R493 --> R494 R494 --> R495 R495 --> R496 R496 --> R497 R497 --> R498 R498 --> R499 R499 --> R500 R500 --> R501 R501 --> R502 R502 --> R503 R503 --> R504 R504 --> R505 R505 --> R506 R506 --> R507 R507 --> R508 R508 --> R509 R509 --> R510 R510 --> R511 R511 --> R512 R512 --> R513 R513 --> R514 R514 --> R515 R515 --> R516 R516 --> R517 R517 --> R518 R518 --> R519 R519 --> R520 R520 --> R521 R521 --> R522 R522 --> R523 R523 --> R524 R524 --> R525 R525 --> R526 R526 --> R527 R527 --> R528 R528 --> R529 R529 --> R530 R530 --> R531 R531 --> R532 R532 --> R533 R533 --> R534 R534 --> R535 R535 --> R536 R536 --> R537 R537 --> R538 R538 --> R539 R539 --> R540 R540 --> R541 R541 --> R542 R542 --> R543 R543 --> R544 R544 --> R545 R545 --> R546 R546 --> R547 R547 --> R548 R548 --> R549 R549 --> R550 R550 --> R551 R551 --> R552 R552 --> R553 R553 --> R554 R554 --> R555 R555 --> R556 R556 --> R557 R557 --> R558 R558 --> R559 R559 --> R560 R560 --> R561 R561 --> R562 R562 --> R563 R563 --> R564 R564 --> R565 R565 --> R566 R566 --> R567 R567 --> R568 R568 --> R569 R569 --> R570 R570 --> R571 R571 --> R572 R572 --> R573 R573 --> R574 R574 --> R575 R575 --> R576 R576 --> R577 R577 --> R578 R578 --> R579 R579 --> R580 R580 --> R581 R581 --> R582 R582 --> R583 R583 --> R584 R584 --> R585 R585 --> R586 R586 --> R587 R587 --> R588 R588 --> R589 R589 --> R590 R590 --> R591 R591 --> R592 R592 --> R593 R593 --> R594 R594 --> R595 R595 --> R596 R596 --> R597 R597 --> R598 R598 --> R599 R599 --> R600 R600 --> R601 R601 --> R602 R602 --> R603 R603 --> R604 R604 --> R605 R605 --> R606 R606 --> R607 R607 --> R608 R608 --> R609 R609 --> R610 R610 --> R611 R611 --> R612 R612 --> R613 R613 --> R614 R614 --> R615 R615 --> R616 R616 --> R617 R617 --> R618 R618 --> R619 R619 --> R620 R620 --> R621 R621 --> R622 R622 --> R623 R623 --> R624 R624 --> R625 R625 --> R626 R626 --> R627 R627 --> R628 R628 --> R629 R629 --> R630 R630 --> R631 R631 --> R632 R632 --> R633 R633 --> R634 R634 --> R635 R635 --> R636 R636 --> R637 R637 --> R638 R638 --> R639 R639 --> R640 R640 --> R641 R641 --> R642 R642 --> R643 R643 --> R644 R644 --> R645 R645 --> R646 R646 --> R647 R647 --> R648 R648 --> R649 R649 --> R650 R650 --> R651 R651 --> R652 R652 --> R653 R653 --> R654 R654 --> R655 R655 --> R656 R656 --> R657 R657 --> R658 R658 --> R659 R659 --> R660 R660 --> R661 R661 --> R662 R662 --> R663 R663 --> R664 R664 --> R665 R665 --> R666 R666 --> R667 R667 --> R668 R668 --> R669 R669 --> R670 R670 --> R671 R671 --> R672 R672 --> R673 R673 --> R674 R674 --> R675 R675 --> R676 R676 --> R677 R677 --> R678 R678 --> R679 R679 --> R680 R680 --> R681 R681 --> R682 R682 --> R683 R683 --> R684 R684 --> R685 R685 --> R686 R686 --> R687 R687 --> R688 R688 --> R689 R689 --> R690 R690 --> R691 R691 --> R692 R692 --> R693 R693 --> R694 R694 --> R695 R695 --> R696 R696 --> R697 R697 --> R698 R698 --> R699 R699 --> R700 R700 --> R701 R701 --> R702 R702 --> R703 R703 --> R704 R704 --> R705 R705 --> R706 R706 --> R707 R707 --> R708 R708 --> R709 R709 --> R710 R710 --> R711 R711 --> R712 R712 --> R713 R713 --> R714 R714 --> R715 R715 --> R716 R716 --> R717 R717 --> R718 R718 --> R719 R719 --> R720 R720 --> R721 R721 --> R722 R722 --> R723 R723 --> R724 R724 --> R725 R725 --> R726 R726 --> R727 R727 --> R728 R728 --> R729 R729 --> R730 R730 --> R731 R731 --> R732 R732 --> R733 R733 --> R734 R734 --> R735 R735 --> R736 R736 --> R737 R737 --> R738 R738 --> R739 R7</pre> | | | |

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publant des demandes internationales en vertu du PCT.

| | | | | | | | |
|----|---------------------------|----|--|----|---------------------------------------|----|-----------------------|
| AL | Albanie | ES | Espagne | LS | Lesotho | SI | Slovénie |
| AM | Arménie | FI | Finlande | LT | Lituanie | SK | Slovaquie |
| AT | Autriche | FR | France | LU | Luxembourg | SN | Sénégal |
| AU | Australie | GA | Gabon | LV | Lettonie | SZ | Swaziland |
| AZ | Azerbaïjan | GB | Royaume-Uni | MC | Monaco | TD | Tchad |
| BA | Bosnie-Herzégovine | GE | Géorgie | MD | République de Moldova | TG | Togo |
| BB | Barbade | GH | Ghana | MG | Madagascar | TJ | Tadjikistan |
| BE | Belgique | GN | Guinée | MK | Ex-République yougoslave de Macédoine | TM | Turkménistan |
| BF | Burkina Faso | GR | Grèce | ML | Mali | TR | Turquie |
| BG | Bulgarie | HU | Hongrie | MN | Mongolie | TT | Trinité-et-Tobago |
| BJ | Bénin | IE | Irlande | MR | Mauritanie | UA | Ukraine |
| BR | Brésil | IL | Israël | MW | Malawi | UG | Ouganda |
| BY | Bélarus | IS | Islande | MX | Mexique | US | Etats-Unis d'Amérique |
| CA | Canada | IT | Italie | NE | Niger | UZ | Ouzbékistan |
| CF | République centrafricaine | JP | Japon | NL | Pays-Bas | VN | Viet Nam |
| CG | Congo | KE | Kenya | NO | Norvège | YU | Yougoslavie |
| CH | Suisse | KG | Kirghizistan | NZ | Nouvelle-Zélande | ZW | Zimbabwe |
| CI | Côte d'Ivoire | KP | République populaire démocratique de Corée | PL | Pologne | | |
| CM | Cameroun | KR | République de Corée | PT | Portugal | | |
| CN | Chine | KZ | Kazakhstan | RO | Roumanie | | |
| CU | Cuba | LC | Sainte-Lucie | RU | Fédération de Russie | | |
| CZ | République tchèque | LI | Liechtenstein | SD | Soudan | | |
| DE | Allemagne | LK | Sri Lanka | SE | Suède | | |
| DK | Danemark | LR | Liberia | SG | Singapour | | |
| EE | Estonie | | | | | | |

PROCEDE DE SECURISATION DE DONNEES METTANT EN OEUVRE UN ALGORITHME CRYPTOGRAPHIQUE

5 La présente invention concerne un procédé de sécurisation de données, destiné par exemple à être mis en oeuvre par le microprocesseur d'une carte bancaire ou une carte d'autorisation d'accès lors d'une connexion à un terminal informatique d'authentification.

10 Les procédés de sécurisation de données de type connu mettent en oeuvre un algorithme cryptographique comprenant des cycles d'exécution d'opérations répétitives de traitement d'éléments de données contenus dans une mémoire de la carte pour élaborer une information chiffrée destinée à être communiquée au terminal informatique.

15 L'exécution du procédé par le microprocesseur de la carte engendre l'émission de signaux dérivés tels que des pics de consommation au niveau de l'alimentation électrique du microprocesseur, ou des variations du rayonnement électromagnétique de sorte que l'enveloppe du rayonnement électromagnétique est significative des données traitées. Un fraudeur désirant utiliser de façon non autorisée les cartes à microprocesseur peut lancer à plusieurs reprises l'exécution du procédé et 20 analyser les signaux dérivés émis pour établir des correspondances entre les différentes opérations de traitement et chaque signal ou série de signaux. A partir de ces correspondances, et en soumettant par exemple la carte à des perturbations électromagnétiques ou des baisses de tension à des instants précis du déroulement de l'algorithme, le fraudeur peut étudier l'information chiffrée obtenue et les différences, 25 ou au contraire l'absence de différences, entre les signaux dérivés émis pour découvrir les données contenues dans la mémoire de la carte.

30 Pour compliquer une telle analyse des signaux dérivés, on a pensé à engendrer des signaux parasites venant s'ajouter aux signaux dérivés émis lors de l'exécution du procédé. L'extraction des signaux correspondant à l'exécution du procédé est alors plus délicate mais demeure possible. On a également pensé à concevoir les composants électroniques de la carte et le programme d'exécution du procédé de sorte que les signaux dérivés émis soient indépendants de la valeur des données sensibles.

Toutefois, ceci complique la réalisation des cartes sans assurer une protection satisfaisante des données.

Un but de l'invention est de proposer un procédé de sécurisation efficace ne présentant pas les inconvénients précités.

5 En vue de la réalisation de ce but, on prévoit, selon l'invention, un procédé de sécurisation de données mettant en oeuvre un algorithme cryptographique d'exécution d'opérations de traitement d'éléments de données pour élaborer une information chiffrée, ce procédé comprenant au moins une étape de transformation aléatoire de l'exécution d'au moins une opération d'un cycle à un autre ou de
10 transformation aléatoire d'au moins un des éléments de données de telle sorte que l'information chiffrée soit inchangée par cette transformation aléatoire.

15 Par transformation aléatoire de l'exécution d'au moins une opération, on entend une modification de l'ordre d'exécution d'opérations ou de parties d'opérations, ou une modification du déroulement d'une seule opération. Ainsi, au moins une opération et/ou au moins une des données traitées sont modifiées aléatoirement, ce qui affecte de façon aléatoire les signaux dérivés émis. Il est de ce fait très difficile pour un fraudeur de distinguer les différentes opérations de traitement et de découvrir les données à partir des signaux dérivés. En outre, la modification aléatoire n'affecte pas l'information chiffrée de sorte que celle-ci peut être utilisée de façon habituelle après
20 son élaboration.

D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description qui suit d'un mode de mise en oeuvre particulier non limitatif de l'invention, en relation avec la figure unique annexée illustrant sous forme d'un schéma par blocs le déroulement du procédé selon ce mode de mise en oeuvre.

25 Le procédé de sécurisation selon l'invention est ici décrit mettant en oeuvre un algorithme cryptographique symétrique de type DES (abréviation des termes DATA ENCRYPTION STANDARD) en vue d'élaborer une information chiffrée C de 64 bits à partir d'un bloc message M et d'une clé secrète K1 eux-mêmes de 64 bits.

Le procédé débute par la permutation 10 des bits du bloc message M
30 entre eux pour former le bloc M0.

Le bloc M0 est alors divisé en deux blocs M1 et M2 de 32 bits lors d'une étape de division 20.

Il est ensuite procédé à l'expansion 30 du bloc M2 pour former un bloc M3 de 48 bits. Cette expansion 30 est par exemple réalisée en découpant le bloc M2 en huit quartets et en ajoutant à chaque quartet le bit extrême adjacent des quartets encadrant le quartet concerné (les quartets extrêmes étant considérés comme 5 adjacentes).

Parallèlement à ces opérations, une permutation 110 est effectuée sur les bits de la clé K1 pour former la clé K2. Les bits non significatifs de la clé K1 sont simultanément supprimés de sorte que la clé K2 a seulement 56 bits.

Selon l'invention, les bits de la clé K2 sont alors modifiés aléatoirement 10 lors d'une transformation 120. Les bits de la clé K3 correspondant aux bits modifiés de la clé K2, ici marqués par une étoile, sont mémorisés. La transformation aléatoire 120 est par exemple réalisée en associant à la clé K2, par l'intermédiaire d'un opérateur logique de type OU exclusif, un nombre aléatoire engendré par un générateur de nombres non prédictibles de la carte.

15 Une clé K4 est obtenue par la rotation 130 des bits de la clé K3. Puis, une permutation 140 est réalisée sur les bits de la clé K4 pour former la clé K5. Simultanément à la permutation 140, les bits non significatifs de la clé K4 sont éliminés de sorte que la clé K5 comporte 48 bits.

20 Le procédé se poursuit par l'association 210 du bloc M3 et de la clé K5 par l'intermédiaire d'un opérateur logique de type OU exclusif. Le résultat de cette association est le bloc R1.

25 La transformation inverse des bits du bloc R1 correspondant aux bits modifiés par la transformation 120 est ensuite réalisée pour former le bloc R2. Cette transformation 220 inverse de la transformation 120 vise à remettre les bits du bloc R1 correspondant aux bits marqués d'une étoile dans l'état dans lequel ils auraient été en l'absence de la transformation 120.

Il est ensuite procédé, de façon classique, à la division et au traitement 230 du bloc R2, à la permutation 240 des bits du bloc R3 formés lors de l'étape 230, et à l'association 250 du bloc R4 résultat de l'étape 240 au bloc M1 par un opérateur OU 30 exclusif pour former le bloc R5.

Le groupe d'opérations, désigné de manière générale par la référence 270, est ensuite exécuté à nouveau à quinze reprises en affectant, à chacune de celles-ci,

la valeur du bloc M1 au bloc M2 et la valeur du bloc R5 au bloc M1 lors d'une étape d'affectation 260.

Le procédé se termine par l'opération 300 d'obtention de l'information chiffrée C par la permutation inverse et la réunion du bloc dernier M2 et du bloc 5 dernier R5 obtenus.

On comprend que l'étape de modification aléatoire de la clé K2 comprend la phase de transformation 120 et la phase de transformation inverse 220. Ces deux phases permettent d'obtenir une information chiffrée C qui n'est pas affectée par cette modification aléatoire.

10 On pourrait également réaliser de la même manière une modification aléatoire du bloc M2 et/ou d'une autre donnée.

Selon un autre mode de mise en oeuvre de l'invention, lequel peut être associé à une étape de modification telle que précédemment décrite, l'exécution d'au moins une opération peut être modifiée de façon aléatoire d'un cycle à l'autre, un cycle 15 pouvant être un cycle complet d'exécution de l'algorithme ou un cycle intermédiaire d'exécution d'un groupe d'opérations.

Par exemple, une détermination aléatoire de l'ordre d'exécution de certaines opérations peut être réalisée au cours d'un cycle d'exécution de l'algorithme. Les opérations retenues seront celles dont l'ordre d'exécution les unes par rapport aux 20 autres n'influent pas sur le résultat. Pour réaliser cette détermination, on pourra prévoir à la fin des opérations choisies un saut conditionnel vers certaines opérations en fonction de la valeur d'un nombre aléatoire ou définir un tableau des adresses des différentes opérations parcouru de façon aléatoire.

A titre d'exemple, la permutation 10 des bits du bloc message M 25 pourrait être effectuée après la permutation 110 des bits de la clé K1 ou inversement.

De même, il pourrait être prévu une détermination aléatoire de l'ordre d'exécution des opérations du groupe 270 pour chaque cycle intermédiaire d'exécution de celles-ci (16 cycles intermédiaires d'exécution de ces opérations pour un cycle complet d'exécution de l'algorithme). Là encore, l'ordre d'exécution de ces opérations 30 sera choisi pour ne pas influer sur le résultat.

Par ailleurs, pour certaines opérations, les données sont traitées par éléments. Ainsi, lors de l'expansion 30, les blocs M2 sont traités par quartets. Lors de

cette opération, on peut prévoir de déterminer aléatoirement l'ordre de traitement des différents quartets. De même, lors de la permutation 140 les bits de la clé K4 sont traités individuellement. Une étape de détermination aléatoire de l'ordre de traitement des bits peut également être prévue pour l'exécution de cette permutation. Les quartets 5 du bloc M2 peuvent également être traités en alternance avec les bits de la clé K4, c'est-à-dire que l'on traite par exemple un premier quartet du bloc M2 puis une série de bits de la clé K4, puis un deuxième quartet du bloc M2 etc., en mémorisant à chaque fois les éléments de donnée traités afin de contrôler que toutes les opérations requises sont bien exécutées.

10 Bien entendu, l'invention n'est pas limitée au mode de réalisation qui vient d'être décrit, mais englobe au contraire toute variante reprenant, avec des moyens équivalents, ses caractéristiques essentielles.

15 En particulier, bien que l'invention ait été décrite en relation avec un algorithme de type DES, l'invention peut être appliquée à d'autres algorithmes symétriques qui procèdent par modification de bits. Ainsi, la modification étant effectuée au moyen d'un opérateur logique du type OU EXCLUSIF, la longueur des éléments de données non transformés est identique à la longueur de ces éléments de données transformés.

20 De plus, les nombres de bits des données ne sont mentionnés qu'à titre indicatif et peuvent être modifiés pour être adaptés au degré de sécurisation envisagé.

On notera par ailleurs que tous les éléments de données M, M0, M1, M2, M3, K1, K2, K3, K4, K5, R1, R2, R3, R4 et R5 peuvent être transformés en leur associant, par l'intermédiaire de l'opérateur logique OU EXCLUSIF, un nombre aléatoire sachant que, postérieurement à cette étape de transformation aléatoire, on 25 procédera à une étape de transformation inverse de sorte que l'information chiffrée C soit inchangée par lesdites transformations.

En particulier, les éléments de données peuvent être des clés K1, K2, K3, K4, K5 ou des blocs de message M, M0, M1, M2, M3 ou des blocs de messages associés à une clé par un opérateur logique du type OU EXCLUSIF R1, R2, R3, R4, 30 R5.

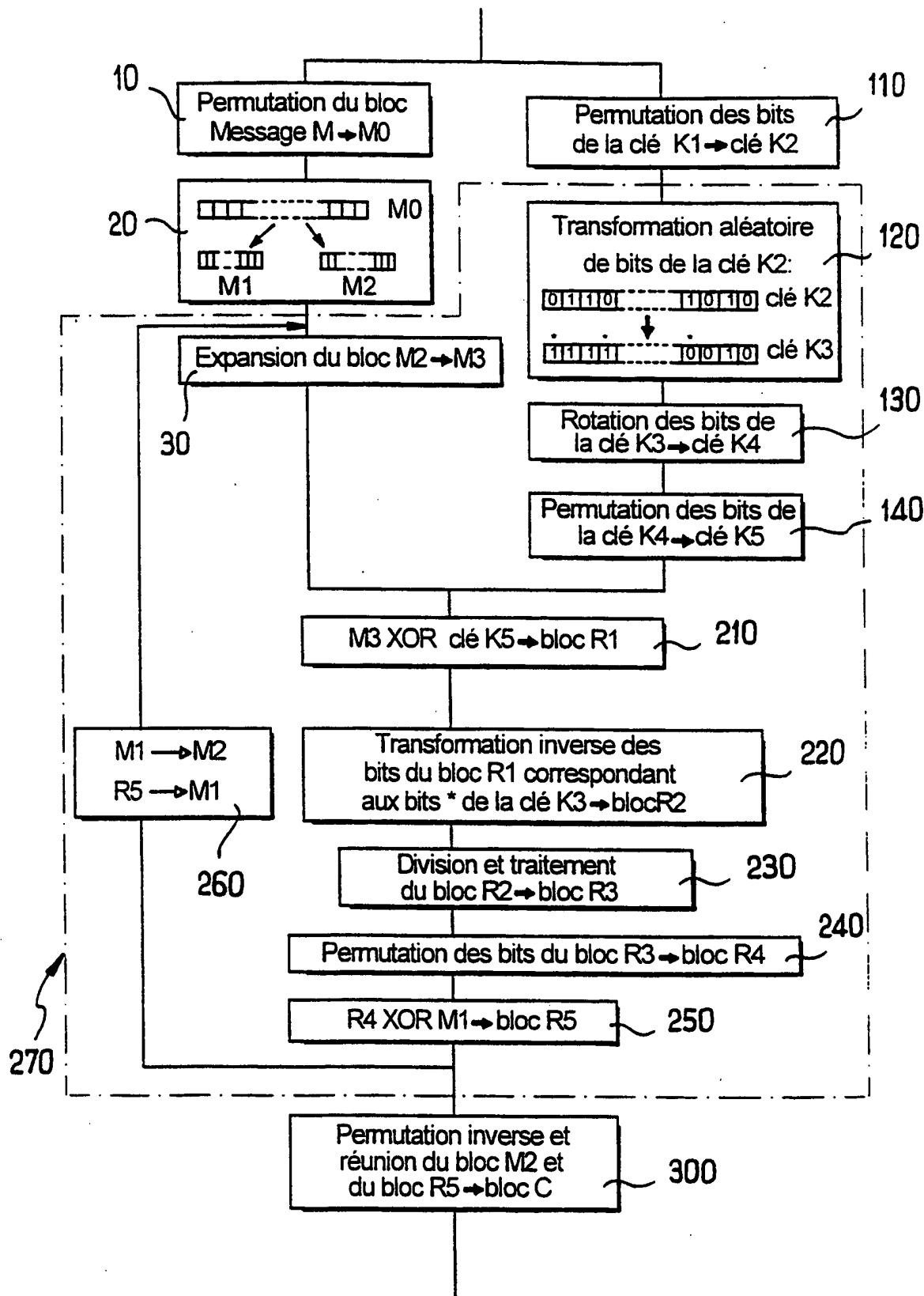
On notera enfin que, si l'étape de transformation aléatoire est une étape préalable au groupe d'opérations exécuté à plusieurs reprises et si l'étape de

transformation inverse est une étape postérieure audit groupe d'opérations, il suffit de générer un nombre aléatoire une fois et de traiter le bloc de message M par l'algorithme pour obtenir une information chiffrée, tous les éléments de données du bloc étant modifiés. La chaîne des données est protégée de bout en bout. En outre, en ne 5 multipliant pas les étapes de transformation et le nombre de nombres aléatoires générés, l'algorithme est mis en oeuvre rapidement, ce qui est nécessaire dans le cas d'une carte à puce où la durée de l'exécution d'un algorithme doit être minimale.

REVENDICATIONS

1. Procédé de sécurisation de données (M) mettant en oeuvre, dans un microprocesseur d'une carte à puce, un algorithme cryptographique d'exécution d'opérations de traitement d'éléments de données (M, M0, M1, M2, M3, K1, K2, K3, K4, K5, R1, R2, R3, R4, R5) pour élaborer une information chiffrée (C), caractérisé en ce qu'il comprend au moins, d'une part, une étape de transformation (120) aléatoire de bits d'au moins un des éléments de données (K2) en associant audit élément de données (K2), par l'intermédiaire d'un opérateur logique du type OU EXCLUSIF, un nombre aléatoire, et, d'autre part, postérieurement à cette étape de transformation aléatoire, une étape de transformation inverse (220), de telle sorte que l'information chiffrée (C) soit inchangée par ces étapes de transformation (120, 220).
2. Procédé de sécurisation selon la revendication 1, caractérisé en ce qu'un élément de données transformé de manière aléatoire est une clé (K1, K2, K3, K4, K5).
3. Procédé de sécurisation selon l'une des revendications 1 ou 2, caractérisé en ce qu'un élément de données transformé de manière aléatoire est un bloc de message (M, M0, M1, M2, M3).
4. Procédé de sécurisation selon l'une des revendications 1, 2 ou 3, caractérisé en ce qu'un élément de données transformé de manière aléatoire est un bloc de message associé à une clé par un opérateur logique du type OU EXCLUSIF (R1, R2, R3, R4, R5).
5. Procédé de sécurisation selon l'une des revendications précédentes, caractérisé en ce que l'algorithme cryptographique d'exécution d'opérations de traitement de données (M, M0, M1, M2, M3, K1, K2, K3, K4, K5, R1, R2, R3, R4, R5) comprend un groupe d'opérations (270) exécuté à plusieurs reprises.
6. Procédé de sécurisation selon la revendication 5, caractérisé en ce que l'étape de transformation aléatoire est une étape préalable au groupe d'opérations (270) exécuté à plusieurs reprises et en ce que l'étape de transformation inverse est une étape postérieure audit groupe d'opérations (270).
7. Procédé de sécurisation selon l'une des revendications précédentes, caractérisé en ce qu'il comprend en outre une étape de modification aléatoire de l'ordre d'exécution des opérations du groupe d'opérations (270).
8. Procédé de sécurisation selon l'une des revendications précédentes, caractérisé

en ce que l'algorithme cryptographique est du type DATA ENCRYPTION STANDARD.



INTERNATIONAL SEARCH REPORT

International Application No

PCT/FR 99/00613

A. CLASSIFICATION OF SUBJECT MATTER
 IPC 6 H04L9/06 H04L9/30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|----------|---|-----------------------|
| A | <p>KOCHER P C: "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems" ADVANCES IN CRYPTOLOGY - CRYPTO'96. 16TH ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE. PROCEEDINGS, SANTA BARBARA, CA, USA, 18-22 AUG. 1996, pages 104-113, XP000626590 ISBN 3-540-61512-1, 1996, Berlin, Germany, Springer-Verlag, Germany see abstract see page 111, line 23 - last line see page 112, paragraph 3</p> <p>-----</p> | 1,5 |

Further documents are listed in the continuation of box C.

Patent family members are listed in annex.

* Special categories of cited documents :

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

T later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

X document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

Y document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

& document member of the same patent family

Date of the actual completion of the international search

Date of mailing of the international search report

15 June 1999

21/06/1999

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
 NL - 2280 HV Rijswijk
 Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
 Fax: (+31-70) 340-3016

Authorized officer

Holper, G

TRAITE DE LA COOPERATION EN MATIERE DE BREVETS

Expéditeur: le BUREAU INTERNATIONAL

PCT

NOTIFICATION D'ELECTION

(règle 61.2 du PCT)

| | |
|---|--|
| Date d'expédition (jour/mois/année) 05 octobre 1999 (05.10.99) | ÉTATS-UNIS D'AMÉRIQUE en sa qualité d'office élu |
| Demande internationale no PCT/FR99/00613 | Référence du dossier du déposant ou du mandataire 76-0481 |
| Date du dépôt international (jour/mois/année) 17 mars 1999 (17.03.99) | Date de priorité (jour/mois/année) 17 mars 1998 (17.03.98) |
| Déposant SALLE, Patrick | |

1. L'office désigné est avisé de son élection qui a été faite:

dans la demande d'examen préliminaire international présentée à l'administration chargée de l'examen préliminaire international le:

02 septembre 1999 (02.09.99)

□ dans une déclaration visant une élection ultérieure déposée auprès du Bureau international le:

2. L'élection a été faite

X

n'a pas été faite

avant l'expiration d'un délai de 19 mois à compter de la date de priorité ou, lorsque la règle 32 s'applique, dans le délai visé à la règle 32.2b).

| | |
|--|--|
| <p>Bureau international de l'OMPI 34, chemin des Colombettes 1211 Genève 20, Suisse</p> <p>no de télécopieur: (41-22) 740.14.35</p> | <p>Fonctionnaire autorisé</p> <p>Kiwa Mpay</p> <p>no de téléphone: (41-22) 338.83.38</p> |
|--|--|

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

| | | |
|--|---|--|
| Référence du dossier du déposant ou du mandataire 76-0481 | POUR SUITE voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après A DONNER | |
| Demande internationale n° PCT/FR 99/ 00613 | Date du dépôt international (jour/mois/année) 17/03/1999 | (Date de priorité (la plus ancienne) (jour/mois/année) 17/03/1998 |
| Déposant SCHLUMBERGER SYSTEMES et al. | | |

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 2 feilles.

Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. **Base du rapport**

a. En ce qui concerne la **langue**, la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.

la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.

b. En ce qui concerne les **séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :

contenu dans la demande internationale, sous forme écrite.

déposée avec la demande internationale, sous forme déchiffrable par ordinateur.

remis ultérieurement à l'administration, sous forme écrite.

remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne vas pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2. Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche (voir le cadre I).

3. Il y a absence d'unité de l'invention (voir le cadre II).

4. En ce qui concerne le **titre**,

le texte est approuvé tel qu'il a été remis par le déposant.

Le texte a été établi par l'administration et a la teneur suivante:

5. En ce qui concerne l'**abrégé**,

le texte est approuvé tel qu'il a été remis par le déposant

le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

6. La figure **des dessins** à publier avec l'abrégé est la Figure n°

suggérée par le déposant.

parce que le déposant n'a pas suggéré de figure.

parce que cette figure caractérise mieux l'invention.

1



Aucune des figures
n'est à publier.

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No

FR 99/00613

A. CLASSEMENT DE L'OBJET DE LA DEMANDE

CIB 6 H04L9/06 H04L9/30

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 6 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

| Catégorie | Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents | no. des revendications visées |
|-----------|--|-------------------------------|
| A | <p>KOCHER P C: "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems" ADVANCES IN CRYPTOLOGY - CRYPTO'96. 16TH ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE. PROCEEDINGS, SANTA BARBARA, CA, USA, 18-22 AUG. 1996, pages 104-113, XP000626590 ISBN 3-540-61512-1, 1996, Berlin, Germany, Springer-Verlag, Germany voir abrégé voir page 111, ligne 23 - dernière ligne voir page 112, alinéa 3 -----</p> | 1,5 |

Voir la suite du cadre C pour la fin de la liste des documents

Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

- "A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- "E" document antérieur, mais publié à la date de dépôt international ou après cette date
- "L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
- "O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
- "P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

15 juin 1999

Date d'expédition du présent rapport de recherche internationale

21/06/1999

Nom et adresse postale de l'administration chargée de la recherche internationale

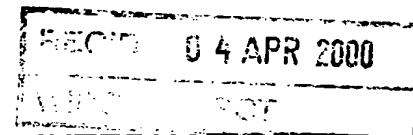
Office Européen des Brevets, P.B. 5818 Patentlaan 2
 NL - 2280 HV Rijswijk
 Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
 Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Holper, G

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT



RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(article 36 et règle 70 du PCT)

| | | |
|--|---|---|
| Référence du dossier du déposant ou du mandataire 76-0481 | POUR SUITE A DONNER | voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416) |
| Demande internationale n° PCT/FR99/00613 | Date du dépôt international (jour/mois/année) 17/03/1999 | Date de priorité (jour/mois/année) 17/03/1998 |
| Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB H04L9/06 | | |
| Déposant SCHLUMBERGER SYSTEMES et al. | | |
| <p>1. Le présent rapport d'examen préliminaire international, établi par l'administration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.</p> <p>2. Ce RAPPORT comprend 5 feuilles, y compris la présente feuille de couverture.</p> <p><input type="checkbox"/> Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).</p> <p>Ces annexes comprennent feuilles.</p> | | |
| <p>3. Le présent rapport contient des indications relatives aux points suivants:</p> <ul style="list-style-type: none"> I <input checked="" type="checkbox"/> Base du rapport II <input type="checkbox"/> Priorité III <input type="checkbox"/> Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle IV <input type="checkbox"/> Absence d'unité de l'invention V <input checked="" type="checkbox"/> Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration VI <input type="checkbox"/> Certains documents cités VII <input checked="" type="checkbox"/> Irrégularités dans la demande internationale VIII <input type="checkbox"/> Observations relatives à la demande internationale | | |

| | |
|--|---|
| Date de présentation de la demande d'examen préliminaire internationale 02/09/1999 | Date d'achèvement du présent rapport 30.03.2000 |
| Nom et adresse postale de l'administration chargée de l'examen préliminaire international: Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465 | Fonctionnaire autorisé Grimaldo, M N° de téléphone +49 89 2399 7513 |



RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

Demande internationale n° PCT/FR99/00613

I. Base du rapport

1. Ce rapport a été rédigé sur la base des éléments ci-après (les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées, dans le présent rapport, comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications.) :

Description, pages:

1-6 version initiale

Revendications, N°:

1-8 version initiale

Dessins, feuilles:

1/1 version initiale

2. Les modifications ont entraîné l'annulation :

- de la description, pages :
- des revendications, n°s :
- des dessins, feuilles :

3. Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

4. Observations complémentaires, le cas échéant :

**RAPPORT D'EXAMEN
PRELIMINAIRE INTERNATIONAL**

Demande internationale n° PCT/FR99/00613

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

| | |
|--|--------------------------|
| Nouveauté | Oui : Revendications 1-8 |
| | Non : Revendications |
| Activité inventive | Oui : Revendications 1-8 |
| | Non : Revendications |
| Possibilité d'application industrielle | Oui : Revendications 1-8 |
| | Non : Revendications |

2. Citations et explications

voir feuille séparée

VII. Irrégularités dans la demande internationale

Les irrégularités suivantes, concernant la forme ou le contenu de la demande internationale, ont été constatées :

voir feuille séparée

Documents mentionnés

Il est fait référence au document suivant:

D1: KOCHER P C: "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems", ADVANCES IN CRYPTOLOGY - CRYPTO'96. 16TH ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE, PROCEEDINGS, SANTA BARBARA, CA, USA, 18-22 AUG. 1996, pages 104-113, XP000626590 ISBN 3-540-61512-1, 1996, Berlin, Germany, Springer-Verlag, Germany

V. Déclaration motivée selon la règle 66.2.a)ii) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. La présente application concerne un procédé (revendication 1) de sécurisation de données.

L'exécution d'opérations avec une carte à microprocesseur comporte l'émission de signaux dérivés tels que des pics de consommation au niveau de l'alimentation électrique du microprocesseur. Un fraudeur peut analyser ces signaux pour les étudier et essayer de dériver les informations chiffrées dans la carte.

La présente invention prévoit d'une part l'exécution d'une transformation aléatoire sur au moins un des éléments des données et d'autre part une transformation inverse tel que l'information chiffrée finale soit inchangée par ces étapes. Ces transformations modifient aléatoirement les données, ce qui affecte de façon aléatoire les signaux dérivés émis. Il est très difficile pour un fraudeur de distinguer les différentes opérations de traitement et de découvrir les données à partir des signaux dérivés.

Une telle solution n'est ni divulguée ni suggérée par l'état de la technique.

Le document D1 considère le même problème de sécurisation de données dans une carte à puce.

Cependant le document propose différentes techniques pour sécuriser les données: il propose soit une technique pour masquer le temps de durée du procédé du microprocesseur d'une façon fixe (page 110, dernier paragraphe) ou d'une façon aléatoire (page 111, lignes 10-11) soit une technique similaire à celle pour masquer une signature digitale (page 111, lignes 23-43).

Toutefois le document D1 ne mentionne pas la possibilité d'utiliser une transformation aléatoire et sa transformation inverse comme dans la présente invention.

La solution proposée dans la revendication 1 de la présente demande est donc considérée comme nouvelle et impliquant une activité inventive (Article 33(1,2,3) PCT).

Les revendications 2-8 dépendent de la revendication 1 et satisfont également aux conditions requises par le PCT en ce qui concerne la nouveauté et l'activité inventive.

VII. Irrégularités dans la demande internationale

1. En vue de remplir les conditions énoncées à la Règle 5.1(a)(ii) PCT, il aurait appartenu au Demandeur de citer dans la description le document D1 et d'indiquer l'état correspondant de la technique.

7
Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

| | | |
|---|---|--|
| Applicant's or agent's file reference, 76-0481 | FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416) | |
| International application No. PCT/FR99/00613 | International filing date (day/month/year) 17 March 1999 (17.03.99) | Priority date (day/month/year) 17 March 1998 (17.03.98) |
| International Patent Classification (IPC) or national classification and IPC H04L 9/06 | | |
| Applicant | SCHLUMBERGER SYSTEMES | |

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 5 sheets, including this cover sheet.

This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of _____ sheets.

3. This report contains indications relating to the following items:

- I Basis of the report
- II Priority
- III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV Lack of unity of invention
- V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI Certain documents cited
- VII Certain defects in the international application
- VIII Certain observations on the international application

| | |
|--|---|
| Date of submission of the demand 02 September 1999 (02.09.99) | Date of completion of this report 30 March 2000 (30.03.2000) |
| Name and mailing address of the IPEA/EP | Authorized officer |
| Facsimile No. | Telephone No. |

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/FR99/00613

I. Basis of the report

1. This report has been drawn on the basis of (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

the international application as originally filed.

the description, pages 1-6, as originally filed,
pages _____, filed with the demand,
pages _____, filed with the letter of _____,
pages _____, filed with the letter of _____.

the claims, Nos. 1-8, as originally filed,
Nos. _____, as amended under Article 19,
Nos. _____, filed with the demand,
Nos. _____, filed with the letter of _____,
Nos. _____, filed with the letter of _____.

the drawings, sheets/fig 1/1, as originally filed,
sheets/fig _____, filed with the demand,
sheets/fig _____, filed with the letter of _____,
sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

the description, pages _____
 the claims, Nos. _____
 the drawings, sheets/fig _____

3. This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

| | | | |
|-------------------------------|--------|-----|-----|
| Novelty (N) | Claims | 1-8 | YES |
| | Claims | | NO |
| Inventive step (IS) | Claims | 1-8 | YES |
| | Claims | | NO |
| Industrial applicability (IA) | Claims | 1-8 | YES |
| | Claims | | NO |

2. Citations and explanations

Reference is made to the following document:

D1: KOCHER P C: "Timing attacks on implementations of Diffie-Hellman, RSA, DSS and other systems", ADVANCES IN CRYPTOLOGY- CRYPTO'96. 16TH ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE, PROCEEDINGS, SANTA BARBARA, CA, USA, 18-22 AUGUST 1996, pages 104-113, XP000626590 ISBN 3-540-61512-1, 1996, Berlin, Germany, Springer-Verlag, Germany

1. The present application relates to a method (Claim 1) for securing data.

Executing operations with a smart card involves the transmission of derived signals such as consumption peaks of the microprocessor's power supply. A defrauder can analyse these signals in order to study them and to try to obtain information encrypted in the card.

The present invention provides for the execution of a random transformation of at least one of the elements of the data and a reverse transformation

such as leaving the final encrypted information unchanged by these steps. These transformations randomly modify the data, which randomly affects the transmitted derived signals. It is very difficult for a defrauder to distinguish the different processing operations and to discover data from derived signals.

Such a solution is not disclosed or suggested by the prior art.

Document D1 considers the same problem of securing data in a chip card.

However, the document proposes different techniques for securing data: it proposes either a technique for hiding the process duration time of the microprocessor in a fixed way (page 110, final paragraph) or randomly (page 111, lines 10 to 11), or a technique similar to that for hiding a digital signature (page 111, lines 23 to 43).

However, document D1 does not mention the possibility of using a random transformation and its reverse transformation as in the present application.

The solution proposed in Claim 1 of the present application is, therefore, considered to be novel and to involve an inventive step (PCT Article 33(1), (2) and (3)).

Claims 2 to 8 depend upon Claim 1 and also fulfil the PCT requirements relating to novelty and inventive step.

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

1. To meet the requirements of PCT Rule 5.1(a)(ii), the applicant should have cited document D1 in the description and indicated the corresponding prior art.